

UNITED STATES DISTRICT COURT

for the
District of Oregon

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

A Samsung Galaxy A21, serial number R9AR20XKH3J, currently located on
the premises of the Federal Bureau of Investigation, Eugene Resident Agency,
Evidence Control Room, in Eugene, Oregon, as further described in
Attachment A

Case No. 6:22-mc-1083

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

A Samsung Galaxy A21, serial number R9AR20XKH3J, currently located on the premises of the Federal Bureau of Investigation, Eugene Resident Agency, Evidence Control Room, in Eugene, Oregon, as further described in Attachment A

located in the _____ District of _____ Oregon _____, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252A(a)(1), (a)(5) and (b)(1)	Possession, receipt, and distribution of visual depictions of minors engaged in sexually explicit conduct and/or child pornography.

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Spencer Anderson, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

Telephone at 2:22pm a.m./p.m. (specify reliable electronic means).

Date: November 18, 2022

City and state: Eugene, Oregon


Judge's signature

Mustafa T. Kasubhai, United States Magistrate Judge

Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF SPENCER J. ANDERSON

**Affidavit in Support of an Application Under Rule 41
for a Warrant to Search and Seize Evidence Including Digital Evidence**

I, Spencer J. Anderson, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since July 2020. My current assignment is to the FBI Portland Division's Eugene Resident Agency. My training and experience include five months of law enforcement and investigative training at the FBI Academy in Quantico, Virginia and law enforcement and investigative work with the Eugene Resident Agency since December 2020. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including Title 18 U.S.C. § 2252A(a)(2), (a)(5), and (b)(1), involving the receipt and possession of child pornography, and I am authorized by law to request a search warrant.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of a Samsung Galaxy A21 smartphone, serial number R9AR20XKH3J (hereinafter the "Device"). The Device is currently stored in law enforcement possession in the Evidence Control Room of the FBI Eugene Resident Agency at 211 E 7th Avenue, Suite 320, Eugene, Oregon 97401. As set forth below, I submit that probable cause exists to believe, and I do believe, that the items set forth in Attachment B constitutes evidence of contraband, fruits, and instrumentalities of violations of Title 18 U.S.C. § 2252A, involving the receipt and possession of child pornography.

Affidavit of SPENCER J. ANDERSON

Page 1
Revised June 2020

3. This affidavit is intended to show only that sufficient probable cause exists for the requested warrant and does not set forth all of my knowledge regarding this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Relevant Statute

4. As set forth below, I submit that probable cause exists to believe, and I do believe, that the Device contains evidence of the following violations:

- Title 18 U.S.C. § 2252A(a)(2), (a)(5), and (b)(1) prohibits knowing receipt or possession of child pornography using any means or facility of interstate commerce, including by computer.

Statement of Probable Cause

Summary

5. During the early months of 2022, Adam Groat (hereinafter “Groat”) was under supervised release of the United States Probation & Pretrial Services Office (USPPSO) for a prior conviction involving the receipt, possession, and distribution of child pornography. Due to this prior conviction, a monitoring application was installed on Groat’s Samsung Galaxy A21 smartphone. The monitoring application detected suspicious activity including, but not limited to, images depicting possible Child Sexual Abuse Material (CSAM) as well as browsing on the “dark web.” On April 11, 2022, Groat was found to have violated conditions of his supervised

release including, but not limited to, possessing materials including visual depictions of minors under the age of 18 engaged in sexually explicit conduct. Groat's U.S. Probation Officer (USPO) subsequently requested assistance from a forensic examiner (hereinafter the "Examiner") to review Groat's smartphone, where the prohibited contents were found. The Examiner's preliminary forensic examination confirmed that the Device was apparently used to access numerous images depicting suspected CSAM and to browse the dark web.

Background and Violation of Supervised Release

6. On September 22, 2016, Adam Michael Groat was sentenced to 84 months in prison for seven counts involving the receipt, possession, and distribution of child pornography in violation of 18 U.S.C. §§ 2252A(a)(1), (a)(2), (a)(5)(B), (b)(1), and (b)(2). Upon release, Groat was to be supervised for a term of life.

7. Special Conditions of Supervision included the following:

a. The defendant shall not view, purchase, or possess any materials including visual depictions of minors under the age of 18 engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2) and (5).

b. The defendant shall submit to a search of the defendant's computer (including any handheld device, any electronic device capable of connecting to any on-line service, or any data storage media) conducted by a U.S. Probation Officer, at a reasonable time and in a reasonable manner, based upon reasonable suspicion of a violation of a condition of supervision.

c. The defendant shall participate in the U.S. Probation Office's Computer Monitoring Program. Participation in the Program may include installation of software or

hardware on the defendant's computer that allows random or regular monitoring of the defendant's computer use; periodic inspection of defendant's computer (including retrieval, copying, and review of its electronic contents) to determine defendant's compliance with the Program; and restriction of the defendant's computer use to those computers, software programs, and electronic services approved by the U.S. Probation Officer.

8. After serving his prison term, Groat was released on supervision. In early 2022, the monitoring application installed on his Samsung Galaxy A21 smartphone detected the suspicious activity mentioned above. This led to the July 2022 forensic examination of the Device.

USPPSO Preliminary Examination

9. The USPPSO Examiner obtained full file system extractions and images of the Device utilizing computer and digital device extraction and imaging tools. The Examiner subsequently conducted a forensic examination of the Samsung smartphone seized from Groat and found that the Device was apparently used to access numerous images depicting suspected CSAM and browse the dark web. The Examiner recovered a large number of cached images depicting CSAM. The images were recovered from different cache folders in the Device's file system.

10. Cached data are files, scripts, images, and other multimedia stored on a device after opening an app or visiting a website for the first time. This data is then used to quickly gather information about the app or website every time revisited, reducing load time. In this case, the presence of these images in cache folders would indicate that the user likely accessed or

viewed the images, which resulted in copies of those images being cached on the system.

11. Provided below are the Examiner's descriptions of four suspected CSAM images. The file names are long, alphanumeric strings that were likely created by the application. The Examiner advised in the report that numerous other suspected CSAM images were recovered in addition to the four listed below:

a. **File Name:**

7556c8a2870548e5aedfd3d35eacf51e3e1cdb81b07e0c5efe59391ac4051018.0; **File Modified Date:** 6/24/2022; **Description:** This image appears to be a screenshot of the mobile device; the browser address bar is visible at the top of the image and the URL *mix.pp.ru* is displayed. (Comment: the .ru TLD means that this website is presumably Russian.) The image depicts what appear to be two prepubescent children, approximately 10-12 years of age, one of whom is a male. They are both in a wooded area and the boy, who is nude, is standing and the other young person, who is partially clothed, is kneeling in front of the boy. The boy's penis is in the mouth of the young person who is kneeling. Smaller images of what appear to be other children are visible at the bottom of the screenshot, as well as the following words in bold letters: "FORBIDDEN K.I.D.S. VIRGINS (5-15)," "Little Veronika (9 yo)," and "FUCKED LITTLE KIDS."

b. **File Name:** 4350846567890332386.0; **File Modified Date:** 6/2/2022;

Description: This image appears to be a screenshot of the mobile device; the browser address bar is visible at the top of the image and the URL *bargast.com.ru* is displayed. This image appears to depict a prepubescent girl, approximately 5-7 years of age, lying on her back. She is nude from the waist down and her legs are spread and upraised so that

her vaginal area is fully exposed to the camera.

c. **File Name:** 7943002753856555466.0; **File Modified Date:** 5/30/2022;

Description: This image appears to be a screenshot of the mobile device; the browser address bar is visible at the top of the image and the URL *live.pp.ru* is displayed. This image depicts what appears to be a young, prepubescent girl, nude from the waist down. Part of her face has been cropped from the image. She is kneeling down and her vaginal area is fully exposed.

d. **File Name:**

2015c6b31ee8f12bb09f2a1e59c0aa2c282f7652a8b4839fe6f4b45b5200117e.0; **File**





Modified Date: 6/24/2022; **Description:** This image appears to be a screenshot of the mobile device; the browser address bar is visible at the top of the image and the URL *doriolov.com.ru* is displayed. This image depicts what appears to be a prepubescent nude girl, approximately 4-6 years of age, who is upside down with her legs upraised and spread apart. Her vaginal area is fully exposed.

12. In addition to discovering suspected CSAM images on the Device, the Examiner also identified browsing activity of interest. On July 26, 2022, the Device user used the Google Chrome web browser app to perform a Google search using the search term “lollporn-browser”. Through cursory online research, the Examiner came to suspect that “lollporn-browser” is associated with websites hosting suspected CSAM material.

13. The Examiner determined that online browsing on the Device using Chrome also indicated the use of Tor. The “Tor network,” or simply “Tor” (an abbreviation for “The Onion Router”), is a special network of computers on the Internet, distributed around the world,

designed to conceal the true internet protocol (IP) addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor is used to access the dark web, which is frequented by criminals to engage in anonymous illicit activity online.

14. The Uniform Resource Locators (URLs) listed below, discovered on the Device and documented by the Examiner, are indicative of online browsing using Tor:

URL	Site Name	Date/Time - UTC+00:00...	Artifact
			
https://miohisgrt5zc3lnog2gr7pqp4gj6qg5mcg6spvjtc74sftdiab7inqd.onion/	Onion Site	5/28/2022 4:06:46 AM	Chrome Logins
http://3bbaaacczcbdddz.onion/	Onion Site		Potential Browser Activity
http://abikogailmonxlz1.onion/	Onion Site		Potential Browser Activity
http://visitorfi5k17q7i.onion/search/	Onion Site		Potential Browser Activity
http://teensfmhowsvpsoygpwbki6ui4hqqd7t4mz65qo6osvklxtaiko645ad.onion/	Onion Site		Potential Browser Activity
http://xgz2jirp2qrm7buko3z73h4cpgvs2r6pnovesvb722gl7jwo2szqxwqd.onion/	Onion Site		Potential Browser Activity
http://teenjbzp6p52xdk2zqaejxwzqx6na5epuhtdnm6gxkn7a2gj7zhjgid.onion/	Onion Site		Potential Browser Activity

These specific artifacts were associated with the Chrome web browsing app as they were located in the following app directory: \data\data\com.android.chrome\app_chrome\Default\. All of the listed URLs have the .onion top-level domain (TLD) name and use a series of alphanumeric strings as part of the web address. The .onion TLD name designates an anonymous onion service, which was formerly known as a “hidden service,” reachable via the Tor network.

15. The Examiner included in his report two attachments documenting “Installed Applications” and “Application Details” from the Google Play Store on the Device. All applications downloaded to the phone from the Google Play Store, including Chrome, were downloaded by a user associated with email address “adammgroat88@gmail.com”, consistent with the name of the owner of the phone, Adam Groat.

Digital Device Background

16. The Device is currently being stored in law enforcement's possession in the Evidence Control Room of the FBI Eugene Resident Agency at 211 E 7th Avenue, Suite 320,

Eugene, Oregon 97401. The device was seized as described above by the USPO. Based on my conversation with the USPPS Examiner, I know that the Device was stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of USPPS. On November 3, 2022, the Device was transferred to the custody of the FBI. The Device was entered into FBI evidence and then transferred to the FBI Eugene Resident Agency, which received the Device on November 4, 2022 and placed it in storage.

17. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Additionally, data that have been viewed via the Internet is typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. I submit that probable cause exists to believe that data once stored on the device will still be stored there because, based on my knowledge, training, and experience, I know that:

a. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of

deleted data in a “swap” or “recovery” file.

b. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

18. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Device because, based on my knowledge, training, and experience, I know:

a. Data on the Device can provide evidence of a file that was once on the Device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other

external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the device at a relevant time. Further, forensic evidence on a device can show how and when the device was accessed or used. Such “timeline” information allows the forensic analyst and investigators to understand the chronological context of access, use, and events relating to the crime under investigation. This “timeline” information may tend to either inculcate or exculpate the device user. Lastly, forensic evidence on a device may provide relevant insight into the device user’s state of mind as it relates to the offense under investigation. For example, information on a device may indicate the user’s motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a “wiping program” to destroy evidence on the device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a computer (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions

about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

Nature of Examination

19. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

20. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the

warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

21. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

22. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

23. If the Device contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

24. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory

evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

25. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

26. Based on the foregoing, I submit that probable cause exists to believe, and I do believe, that the Device described in Attachment A contains evidence of contraband, fruits, and instrumentalities of violations of the above-described crimes, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the Device described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

///

///

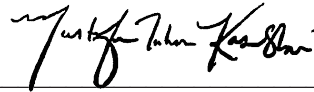
///

27. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) William McLaren, who advised me that in his opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

/s/ Spencer Anderson, per rule 4.1

Spencer J. Anderson
FBI, Special Agent

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 2:22pm
a.m/p.m. on November 18, 2022.



HONORABLE MUSTAFA T. KASUBHAI
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property to be searched is a Samsung Galaxy A21 smartphone, serial number R9AR20XKH3J (hereinafter the “Device”), which is currently stored in law enforcement possession in the Evidence Control Room of the FBI Eugene Resident Agency at 211 E 7th Avenue, Suite 320, Eugene, Oregon 97401.

ATTACHMENT B

Items to Be Seized

1. All records on the Device described in Attachment A that relate to violations of Title 18 U.S.C. § 2252A(a)(2) and (a)(5) and (b)(1) (Receipt and Possession of Child Pornography) and involve Adam Michael Groat from April 1, 2021, through the date of the execution of the search warrant, including:

- a. Any and all records, documents, or materials, including correspondence, that pertain to the production, possession, receipt, or attempt to do so, of images and audio and video recordings of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256, including where such images, audio and video were obtained and how and where they were stored;
- b. All originals and copies of images and audio and video recordings of minors engaged in sexually explicit conduct, as defined in as defined in Title 18, United States Code, Section 2256, and material identifying the minors;
- c. Identifying information, images, video, audio, contact information, addresses, telephone numbers, email addresses, social media site accounts and usernames for persons with whom Garrett traded, purchased, received, sent, or otherwise dealt in Child pornography.
- d. Evidence of the destruction, or attempt to erase, hide or delete the above-described items.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks,

saved usernames and passwords, documents, identifying information and records for accounts, websites social media programs and applications, and browsing history.

3. Records evidencing the use of the Internet, including:
 - a. Records of Internet Protocol addresses used;
 - b. Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - c. Records of data storage accounts and use of data storage accounts;
 - d. Records containing screen names, user names, e-mail addresses and identities assumed for the purposes of communicating on the Internet;
 - e. Internet and cellular data billing and subscriber records.
4. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Search Procedure

5. The examination of the Device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

9. If the Device contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

10. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.